JP 61-264371
11-22-86

DESCRIPTION

1. Title of the Invention

DATA PROTECTION METHOD

2. CLAIMS

(1) A data protection method used in a system where encrypted data is decrypted and used by a data-use apparatus, characterized in that the data-use apparatus is provided with:

decryption means that has a function of decrypting a single piece or some pieces of data encrypted in a plurality of ways when the data is encrypted in the plurality of ways using a plurality of encryption methods and supplied; and

cipher system description means that identifies the single piece or some pieces of the supplied data, i.e., identifies part of the encrypted data which is decryptable by the decryption means.

(2) The data protection method according to claim 1, characterized in that the plurality of encryption methods use the same encryption algorithm but different encryption keys.

(3) The data protection method according to claim 1 or 2, characterized in that the data-use apparatus is provided with a plurality of the decryption means.

(4) A data protection method used in a system where encrypted data is decrypted and used by a data-use apparatus, characterized in that the system is provided with:

decryption means that has a function of, when data encrypted in any desired encryption method and data decryption means information, which describes means for decrypting the encrypted data and includes pieces encrypted in a plurality of ways using a plurality of encryption methods, are supplied, decrypting a single piece or some pieces of the data decryption means information encrypted in the plurality of ways; and

cipher system description means that identifies information part, which is decryptable by the decryption means, of the data decryption means information being encrypted in the plurality of ways.

(5) The data protection method according to claim 4, characterized in that the plurality of encryption methods use the same encryption algorithm but different encryption keys.

(6) The data protection method according to claim 4 or 5, characterized in that the data-use apparatus is provided with a plurality of the decryption means.

3. Detailed Description of the Invention

[Outline]

The present invention relates to a system which delivers encrypted data and allows only a user confirmed as a verified user to use the data by decrypting the encrypted data. The present invention provides means for avoiding risk involved in a case where secret in the decryption method is shared by multiple manufacturers or multiple groups within a company which produce decoders.

[Field of the Industrial Application]

The present invention relates to a protection method for software such as computer programs and videos and for data including deposit balances or the like in a bank.

[Background Art]

In recent years, various paid programs have been on sale along with the development in a data processing system. However, the protection used in the system is not completely secure, and the unauthorized use of programs is increasing.

The same applies to video tapes or data including various kinds of information.

In a case where mass copies of data are made and used in multiple apparatuses as described above, an effective way for preventing the unauthorized use is to allow data to be used only in apparatuses specified by a data supplier.

The basic method for achieving the above way is illustrated in FIG. 6. In a case where data a is provided to data-use apparatuses ① to ⓝ, the data a is encrypted using unique keys K_1 to K_n different

for the respective data-use apparatuses. Accordingly, n pieces of encrypted data ① to ⓝ are created and then delivered to the data-use apparatuses, respectively. Each of the data-use apparatuses exclusively decrypts the supplied data by using the corresponding unique decryption key.

However, with this method, the number of pieces of encrypted data in need of preparation is the same as the number of the data-use apparatuses regardless of the fact that data embodiments have the same content. Therefore, this method is not suitable for mass duplication and mass supply.

[Prior Art]

In the field of computing, a method involving a public-key cryptosystem is proposed as means for protecting supplied computer programs from the unauthorized duplication and use. With this method, a decoder including a decryption key is embedded in a computer. An encryption key corresponding to the decryption key is publicly disclosed to program manufacturers. The program manufacturers encrypt their programs using the encryption key and then distribute the encrypted programs. Each program is decrypted and executed by the decoder in the computer while the decrypted original program is never leaked to the outside from the computer.

Even though the encryption key is publicly disclosed with the public-key cryptosystem, it is virtually impossible to guess the decryption key corresponding thereto. Accordingly, unless the decryption key enclosed in the decoder is leaked to the outside, no one but the manufacturer can know the contents of the program.

Therefore, it is vital to secure the secret of the decryption key in using the method.

[Reference Documents]

1. A. Lempel "Cryptology in Transition" ACM Computing Surveys, Vol. 11. No. 4, pp. 285 - 304

2. M.E. Hellman, translated by Shin Hitotsumatsu, "New Cryptosystem" Nikkei Inc., Science Vol. 19, No. 10, pp. 100 - 112

[Problems to be Solved by the Invention]

A method has been proposed in order to prevent the leakage of the decryption key. With the method, a pair of decryption key and encryption key are automatically generated by a manufacturing apparatus for manufacturing a decoder. Only the encryption key is taken outside as it is while the decryption key is written into the decoder directly by the apparatus, so that the decryption key, as it is, is not exposed to anyone. However, there is a problem that the secrecy with this method is effective only on condition that there is only a single manufacturing apparatus. Thus, this method is not applicable in a case where decoders are produced by multiple manufacturers. Even if there is only a single manufacturer, this method is not applicable in a case where the manufacture uses multiple manufacturing apparatuses.

[Means for Solving the Problems]

An object of the present invention is to overcome the problems in the secrecy of the decryption key described above. What needs to be performed by each company in a case where decoders are

manufactured by multiple companies or by each manufacturing apparatus within a single company is to keep the secret of a key to be enclosed independently in the decoders manufactured by the company or the manufacturing apparatus itself.

The purpose of the present invention would be achieved by means as follows:

1. A part or the whole of data, or a part or the whole of information regarding decode means for an encrypted data would be encrypted in plural way by plural encryption keys or plural encryption methods.

2. A decoder will select one unit among these encrypted data or information that would be appropriate for the decryption key or the decoder thereof.

3. It would be possible to use the encrypted data just by decoding the part of them.

The configuration of the present invention is characterized in that a decoder, including decryption means, further includes means for identifying which encrypted part of data corresponds to a decryption key or the decryption means of the decoder.

FIG. 1 is a diagram illustrating a basic configuration of the present invention.

FIG. (A) illustrates a configuration of encrypted data in a method where contents of data are encrypted in multiple ways using multiple encryption methods, each encrypted data is set as an encrypted block, and then the encrypted blocks are put together and delivered as a line encrypted block. In the example illustrated,

data a is encrypted in n ways, and a line encrypted block including n encrypted blocks is delivered to data-use apparatuses.

FIG. (B) illustrates a configuration of encrypted data in a method where contents of data are encrypted using a single encryption method. The decryption key thereof is encrypted into an encrypted block in multiple ways using multiple encryption methods, and the encrypted blocks are delivered with the encrypted data. In the example illustrated, data, formed of a line encrypted block including n encrypted blocks obtained by encrypting the decryption key in n ways and a single encrypted block obtained by encrypting data a, is delivered to the data-use apparatuses.

FIG. (C) illustrates a configuration of each data-use apparatus: 1 denotes encrypted data; 2 denotes a decoder; 3 denotes cipher system description means; and 4 denotes decryption means.

The encrypted data 1 has a configuration of encryption data as illustrated in FIG. (A) or FIG. (B).

The decoder 2 includes unique cipher system description means 3 and decryption means 4 as a characteristic configuration according to the present invention.

The cipher system description means 3 identifies and acquires the encrypted block that can be decrypted by its decoder from the line encrypted block in the encrypted data 1. The position of the encrypted block in the line encrypted block is previously determined by order in the array or specified by an index. Alternatively, the cipher system description means 3 may identify the corresponding block by trying decryption on all encrypted blocks in turn and determining whether the encrypted blocks are successfully decrypted

or not. The encrypted block acquired from the line encrypted block in the encrypted data 1 is the encrypted data a in case of FIG. (A) and is the encrypted decryption key in case of FIG. (B).

The decryption means 4 performs decryption by applying the decryption key that is unique to the means to the acquired encrypted block. In case of FIG. (A), the outcome of decryption is the data a, and the decryption is completed at this moment. In case of FIG. (B), the outcome of decryption is the decryption key for decrypting the encrypted data a, and the decryption is completed after the decryption means 4 acquires the data a using the decryption key.

[Function]

An example of software is described with reference to a schematic diagram illustrated in FIG. 2.

After developing software (which are represented by marks "□", "△", or "○" in the Figure), software benders provide their products in which at least a part of software has been encrypted in the way of Fig.1 (A) or Fig.1 (B).

Users obtain encrypted software from a distribution channel. A user can copy the software freely, and he can store the software on a certain place of a file system or a network.

However, the software is not available, nor executable unless decryption. Permitted user's computers have decoders comprising Cipher System Description Means 3 and Decryption Means 4. Only software that has been decrypted by the decoder would be executed.

[Embodiment]

Figure 3 shows an embodiment of the system according to the present invention. In the Figure 3, "1" is an encrypted data provided to the system, 1a1-1an are encrypted blocks encrypted by different encryption methods respectively. 1b is an index table (INDEX) that points each head address of the encrypted blocks. 2i and 2j are decoders, which may be produced by different companies. 3i and 3j are Cipher System Description Means, which are inside of 2i and 2j respectively. 4i and 4j are Decryption Means.

When encrypted data 1 is entered in decoder 2i, Cipher System Identification Means 3i reads the index table (INDEX) 1b and determines two matters, 1) among 1a1-1an, which is the encrypted block corresponding to Decryption Means 4i for the decoder 2i, and 2) where is the head address thereof, and sends the information to Decryption Means 4i. Since then, 4i decodes the encrypted data of 1ai and the data would be available.

When encrypted data 1 is entered in decoder 2j, similarly, 1aj is selected among encrypted data 1 and that would be decoded by Decryption Means 4j.

The index table (INDEX) 1b may be spared in a case where each of the encrypted data 1a1 to 1a n is of the same invariable size. Further, the index table (INDEX) 1b may be spared in a case where each header of the encrypted data 1a1 to 1an is a distinctive pattern that can be identified by other units and further identification information on the encrypted block is written into the distinctive pattern.

There is a round-robin method with which decryption is tried

on all encrypted blocks and any block that is successfully decrypted is selected. However, it goes without saying that the decryption may not be successful in some cases depending on a combination of the encrypted data and decryption means.

According to the present invention, the data 1a1 to 1an are encrypted using different encryption methods and decrypted by independent decryption means, respectively. Therefore, in a case where the decoder is produced by multiple companies, these manufactures are no longer required to share the secret of the decryption method.

As a result, the risk of the leakage of the secret of the decryption method is reduced. Furthermore, even if the secret is leaked and the use of the encryption method is suspended, it is possible to minimize damage since not all decoders need to be replaced.

A data supplier can choose any desired encryption method for encrypting data from multiple methods. Depending on the choice, the data supplier can specify the decoder that can access the data. Thus, the data supplier may make the data not to be accessed by some encryption apparatuses produced by companies with unfavorable factors to the data supplier such as a factor that the protection of the secret of the encryption is not secure. In consequence, manufacturers of the decoder make effort to provide more secure protection.

When a public-key cryptosystem is used as the encryption method, the encryption key and the decryption key are different, and it is virtually impossible to guess the decryption key from

the encryption key. Accordingly, in a case where the pair of the encryption key and the decryption key are created by the manufacturer of the decoder, and where the decryption key is enclosed in the decoder and kept as a secret while only the encryption key is handed to the data supplier, the secrecy of the decryption key becomes more easy and secure.

FIG. 4 is an explanatory diagram of another embodiment system of the present invention.

In FIG. 4, the same numerals as FIG. 3 denote the same components. Of the numerals only shown in FIG. 4, 1a denotes encrypted data embodiment, 1b' denotes an index table (INDEX) indicating headers of the encrypted blocks 1d1 to 1dn, 1c denotes information on means for decrypting the data 1a, 1d1 to 1dn denote encrypted blocks obtained by encrypting 1c in different ways, 5i denotes first decryption means for decrypting the encrypted block 1d1, and 6i denotes second decryption means for decrypting the encryption of the contents of data.

Operations are described next with reference to a flowchart in FIG. 5.

When data 1 is inputted to the decoder 2i, the cipher system description means 3i reads the index table (INDEX) 1b'. As a result, the cipher system description means 3i identifies which block of encrypted blocks 1di to 1dn can be decrypted using the decryption means 5i. If the identified block is 1di, the encrypted block 1di is read and decrypted in the first decryption means 5i. The decryption means information 1c for decrypting contents of data is thereby acquired and inputted to the second decrypting means

6i. Then, the second decryption means 6i reads the data embodiment 1a and decrypts the data embodiment 1a according to the decryption means information 1c.

Performing the encryption in two steps allows employing the following encryption method at the first step, i.e., for the encrypted block obtained by encrypting the data indicating means for decrypting the data embodiment, and thereby strengthening the security. Specifically, the encryption method is highly secure but not suitable for encrypting mass data because it takes a long time to perform the decryption.

The encryption of the data embodiment is performed using an encryption method with high decryption speed. Even if the encryption method is not very secure, the encryption method can be set different for each data. The damage of the leakage is thus relatively small compared with the encryption method of the first step.

When a part of data needs even greater protection, the part may not be stored in 1a like other data and may be stored in 1d1 to 1dn with the decryption means data for decrypting the data embodiment. By adopting such a method, the security can be further strengthened.

In the embodiment in FIG. 3, hardware such as ICs in the decoder may previously enclose the internal information needed for the cipher system description means 3i to acquire the encrypted block 1ai corresponding to its own apparatus from the encrypted data 1, and decryption key needed for the decryption means 4i to decrypt the acquired encrypted block 1ai. The same applies to the

cipher system description means 3i and the first decryption means 5i in the embodiment illustrated in FIG. 4.

By enclosing the process routine of the cipher system description means or the decryption means in ICs or the like in the decoder, right to use software can be checked or software can be decrypted without causing ordinary programs to be aware. Alternatively, the process routine may be included in OS while the decryption key or the like may be enclosed in ICs or the like in the CPU in a manner such that the decryption key may be referred to by OS.

[Effects of the Invention]

As described above, according to the present invention, from viewpoint of the manufacturers producing a decoder, the secret of the decryption key enclosed in the decoder needs to be protected only within the company or for each manufacturing apparatus. Thus, it is no longer necessary to share the secret of the decryption key among the manufacturers producing decoders of the same type. Furthermore, it is no longer necessary to let the key be exposed to the outside of the apparatus in order to deliver the key to multiple apparatuses using the same key.

As a result, the risk of secret leakage is reduced, and the reliability on the entire system is improved. Further, cost for the secrecy can be reduced, and the decoder can be produced by multiple companies at their will. As a result, free competition is practiced.

Single data can be encrypted in multiple ways using multiple

keys, so that there may be multiple types of the decoders including different decryption keys. Therefore, even if a single decryption key is leaked and stopped being used, only the decoder corresponding to the decryption key needs to be replaced, and not all decoders need to be replaced. This minimizes the damage.

The data supplier can specify any decoder that can use the data. In consequence, the manufacturers of the decoders make effort to provide more secure protection of the encryption method and data embodiments in order to let more data suppliers use their decoders.

The present invention can be applied to all kinds of information that needs protection, e.g., paid computer programs, paid video software, credit data in a credit card, and the like.

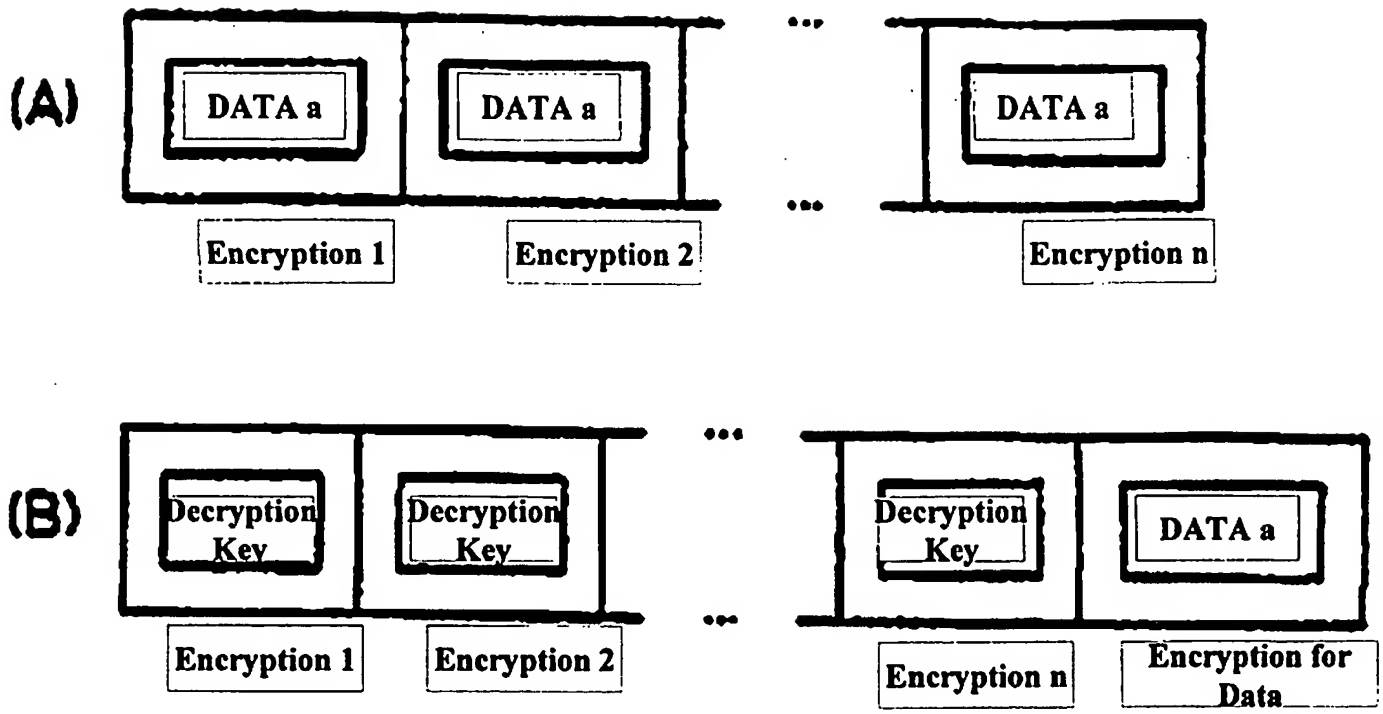
The greatest effect of the present invention is the introduction of competition in the field of data protection in terms of quality enhancement and cost reduction. The competition is substantially the same as the free competition, which is taken for granted in the trading of corporeal products and invokes quality enhancement and cost reduction.

4. Brief Description of the Drawings

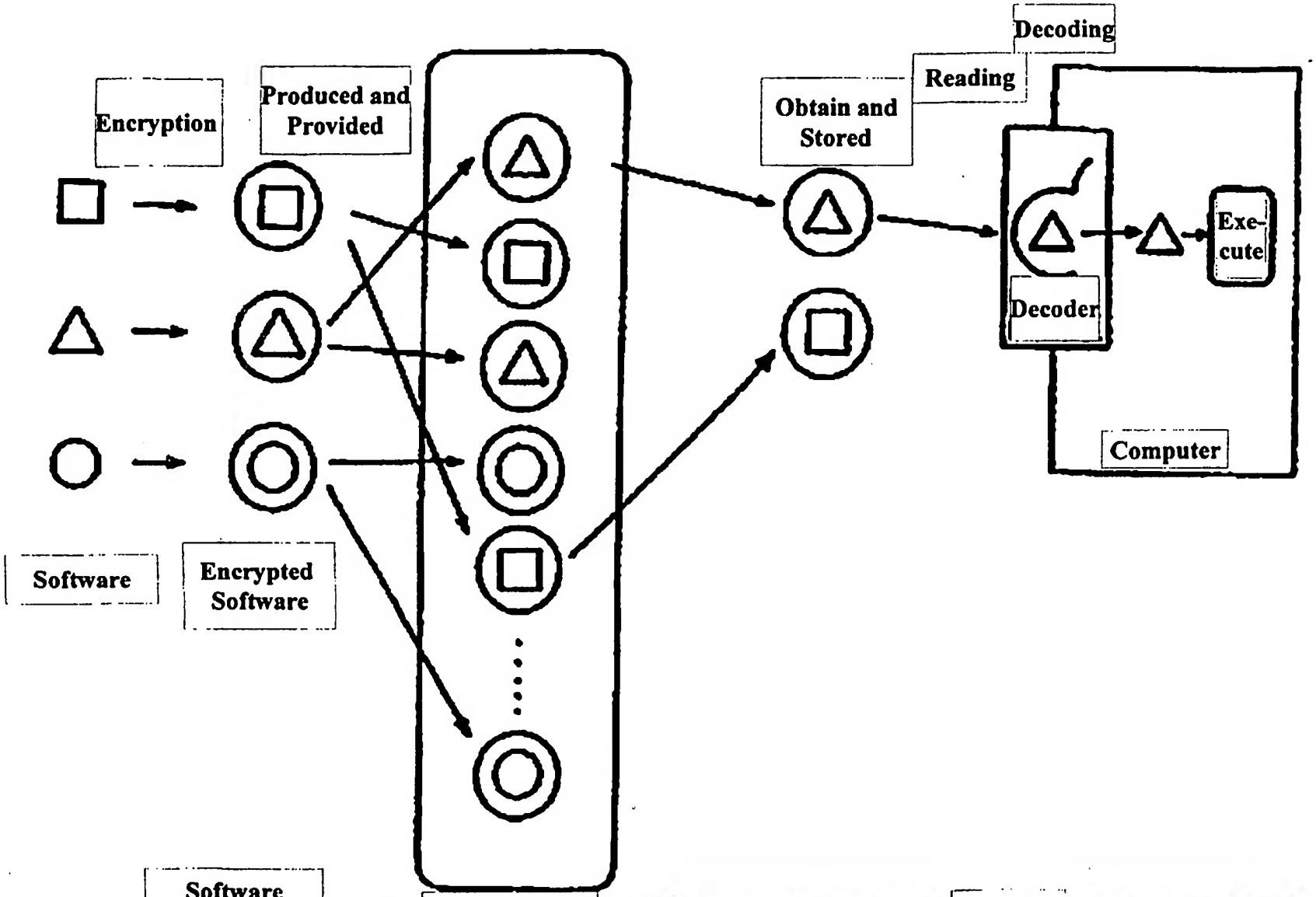
FIG. 1 is a diagram illustrating a basic configuration of the present invention. FIG. 2 is a schematic diagram illustrating a function of the present invention. FIGS. 3 and 4 are explanatory diagrams of the different embodiment systems of the present invention, respectively. FIG. 5 is a flowchart of the embodiment system in FIG. 4. FIG. 6 is an explanatory diagram of the basic

data protection.

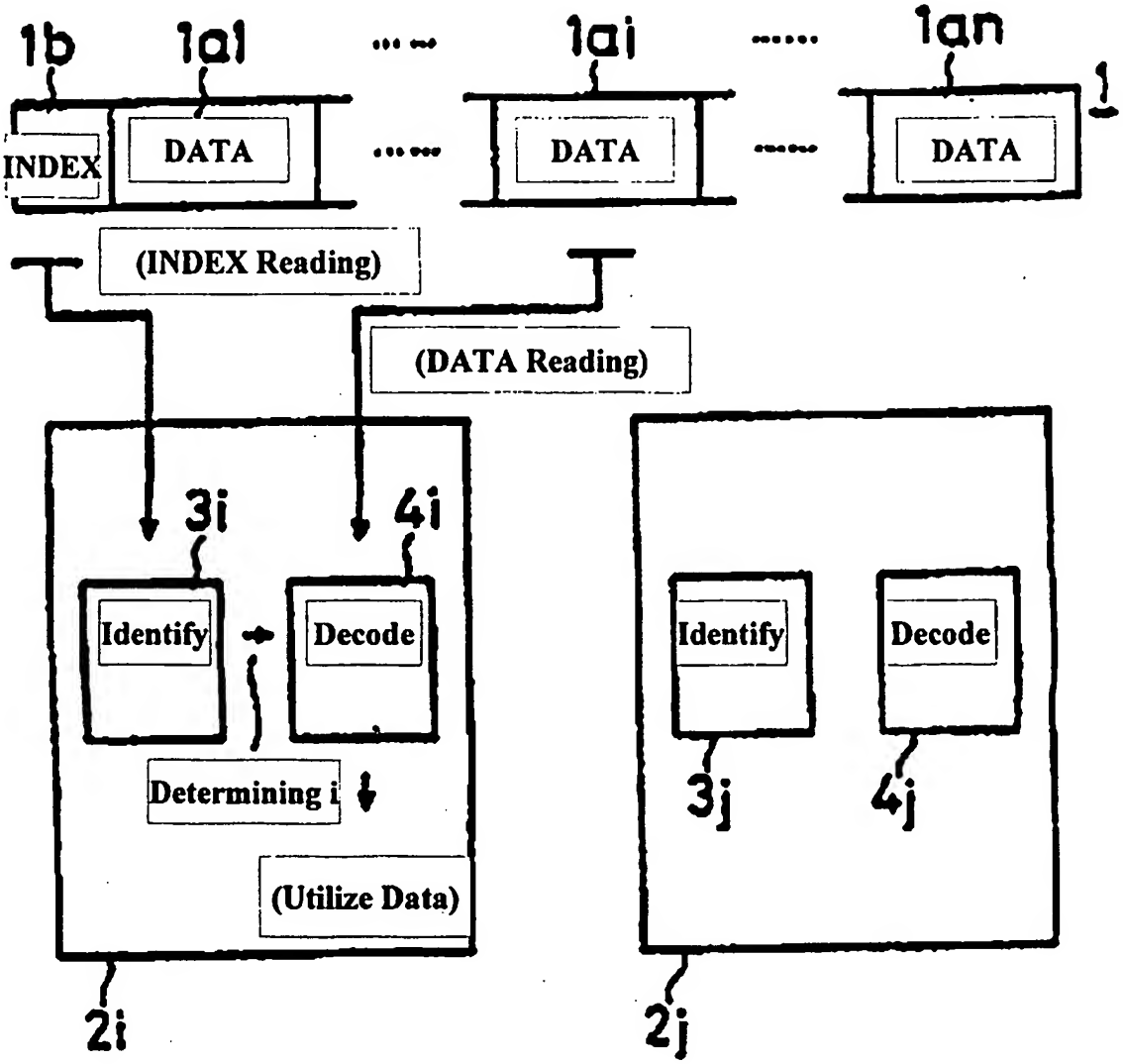
In FIG. 1, 1 denotes encrypted data, 2 denotes a decoder, 3 denotes cipher system description means, and 4 denotes decryption means.



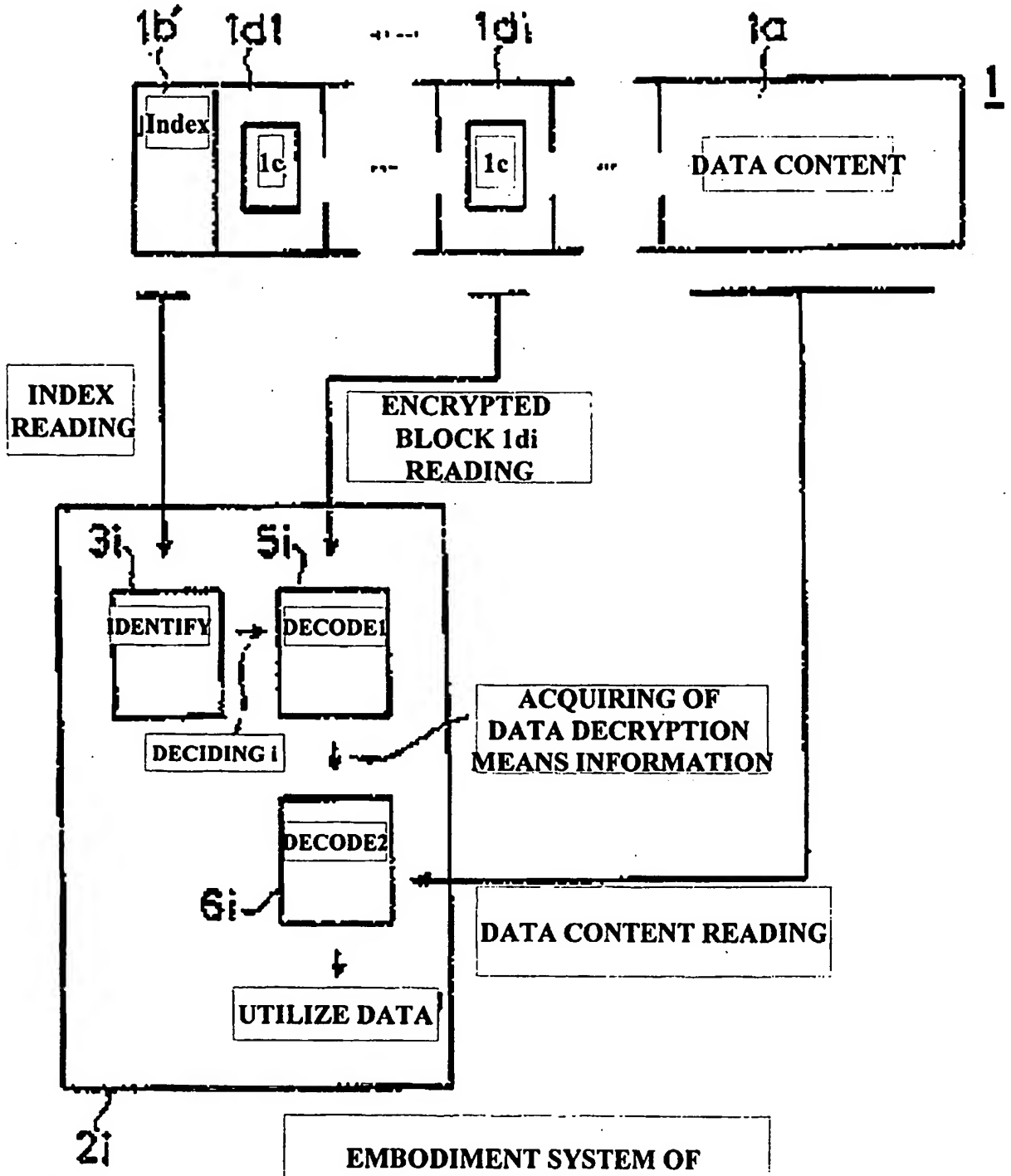
The basic composition of the present invention
Fig. 1



Concept of the present invention
Fig. 2

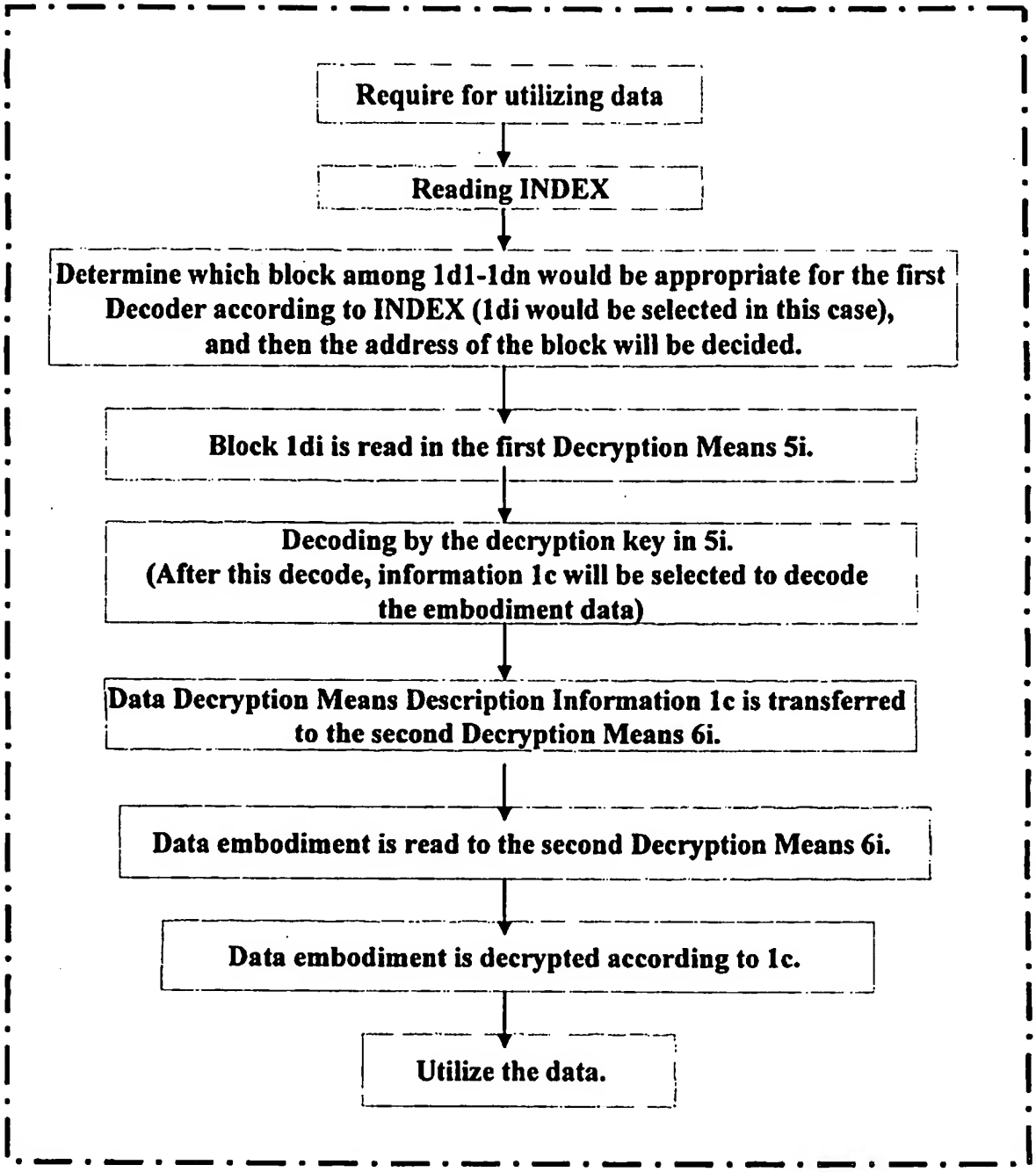


Embodiment system of the present invention
Fig. 3



EMBODIMENT SYSTEM OF THE PRESENT INVENTION

Fig. 4



Flow chart of the embodiment
Fig. 5

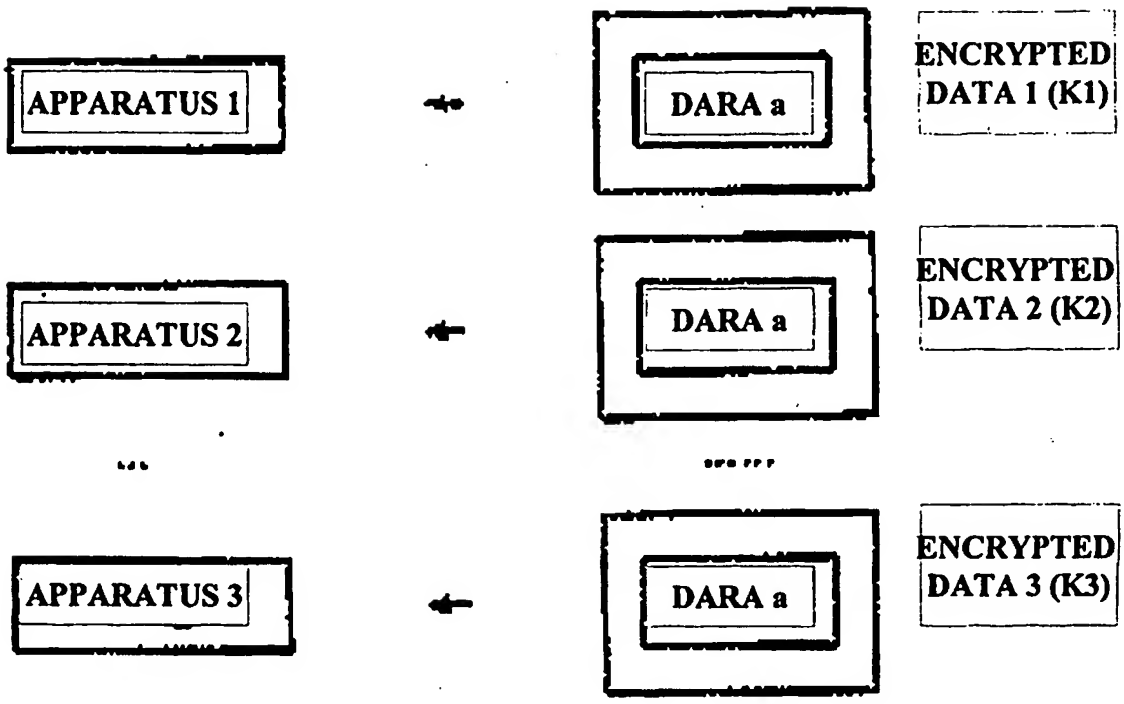


ILLUSTRATION OF BASIC DATA PROTECTION

Fig. 6